WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Study on Cyber Crime Victims

[1]P. Naveen Prabhu, [2]K. Niranjana

[1]Department:BA Llb (Hons), Saveetha School of Law, Saveetha University, Saveetha Institute of Medical and Technical Sciences(SIMATS) Chennai-77, E-Mail I'd:naveenprabhu001.pnp@gmail.com,

[2]Assistant Professor, Saveetha School of Law,Saveetha Institute of Medical And Technical Sciences(SIMATS), Saveetha University, Chennai-77, E-Mail I'd:niranjanak.ssl@saveetha.com,Cell:8695132922

ABSTRACT:

The cyberspace is a large area in which most of the countries are not taking concern in cybercrime and cyber security.so Cyber Crimes are increasing in a steady manner in which victims are individuals who are subjected to cyberattack or cybercrime.Cybercrime Is a crime that involves a computer and a network as medium of offence in the process of crime.The crime may take place on an individual or group or association but this all comes under the preview of cybercrime or cyber attack. this paper mainly focus on cybercrime victims and rules protecting cybercrime victims from mental harassment and psychological issues.cybercrime victims are affected both mentally and financially, which sometimes may led to suicides and other forms of depression they face in their life's every day..the aim of the study is to know about the cyber crime victims and their problems to overcome the attack they meet.the data was collected using simple random sampling method from 1597 people and the secondary sources used are books of various authors and articles on cybercrime and threats in various articles by which we have came to a conclusion that cybercrime victims are being subjected to high level mental problems and they are not been given any care by the government for redevelopment.the laws on cybercrime are not been very effective and still governments are not able to tackle cyberthreats to the internet users who are targets for hackers to loot the identities of persons or thefts involving bank cards and social media harassment issues through cyberspace as medium.

Keywords: Cybercrime, Victims,Hacking, Cyber Security, Cyberbullying.

INTRODUCTION:

The cyber is vast area in which no one can be found for their cyber offence easily.still the government's are lacking behind to take large steps against cyber criminals and cyber crime.the cybercrime consists of victims affected both mentally and financially.the government should want to take steps to improve the cyberspace. We're still the government's are lacking their way back behind.cyber victims should get attention and love should not be bullied instead should want to get help and support to rebuild their life 's.the government should also consider them as victims and vulnerable.the people are aware of their rights the victims are still not fighting back for their rights.the most of the victims are going to commit suicide or runaway from their life's mostly women.Based on cybercrime limitations, the type of cybercrime can be multiform(Pandey n.d.; Imran n.d.). Regarding the target/object(Pandey n.d.; Imran n.d.; Abidi & Abidi 2018; Kumar & Vijaya Kumar 2016), it can be occurred to individuals and society, as well as the government(Abidi & Abidi 2018). A Cybercrime with the individual victims, can be a fraud through online purchasing, including carding actions for victimization carried out by a person or group of people by using another person's credit card that is carried out by violating the law with the support of digital documents(Wright et al. 2017), computers and internet(Damle 2012; Anon 2016) .Cybercrime with corporate as the victim occurs toward corporations in the banking sector or various fields of public(Brown et al. 2018) services(Deshpande et al. 2018; Graham 2018). In the online-based transportation business there are corporations that have become victims of their business partners in this case several online motorcycle taxi drivers who commit fraud by carrying out fictitious orders or transactions which are popularly known as "tuyul". (Abidi & Abidi 2018; Djanggih 2018).Psychological detriment for cybercrime can be experienced by a victim such as harassment, flaming(Jaishankar 2011), denigration, impersonation, outing, cyber stalking(Khan et al. 2017; Anon 2016; Kravetz 2013). Harassment is done by sending the disturbing messages by using email, SMS, or text messages on social media continuously(Halder & Jaishankar 2016). Flaming can be expressed by sending a text messages which the content is full of anger and frontal(Kumar & Vijaya Kumar 2016). Denigration is an act against a person by spreading his ugliness on the internet, especially social media(Walleyn 2009), which intends to damage the reputation of someone's dignity(Deshpande et al. 2018; Wright et al. 2017). crime.Based on cybercrime limitations(Halder & Jaishankar 2016), the type of cybercrime can be multiform(Graham 2018). Regarding the target/object, it can be occurred to individuals and society, as well as the government(Kumar & Vijaya Kumar 2016). A Cybercrime with the individual victims(Kumar & Vijaya Kumar 2016), can be a fraud through online purchasing(Graham 2018), including carding actions for victimization carried out by a person or group of people by using another person's credit card(Martellozzo & Jane 2017; Halder & Debarati 2011; Gandhi & India 2006) that is

[1] Naveen Prabhu 4th year saveetha school of law chennai naveenprabhu001.pnp@gmail.com
Contact no:9940903255

[2] K.Niranjana assistant professor saveetha school of law chennai niranjanak.ssl@saveetha.com
Contact no:8695132922

carried out by violating of the law with the support of digital documents, computers and internet(Fatima et al. 2017).**The aim** of the study is to know about the victims of cyber crime and their problems.

OBJECTIVE:

- To know about the laws protecting women from cyberattacks
- To know about the policies helping cyber crime victims

REVIEW OF LITERATURE:

Elena Martellozzo, Emma A Jane The last twenty years have seen an explosion in the development of information technology, to the point that people spend a major portion of waking life in online spaces. While there are enormous benefits associated with this technology, there are also risks that can affect the most vulnerable in our society but also the most confident. Cybercrime and its victims explores the social construction of violence and victimisation in online spaces and brings together scholars from many areas of inquiry, including criminology, sociology, and cultural, media, and gender studies.Crime is undergoing a metamorphosis.**Routledge**,The online technological revolution has created new opportunities for a wide variety of crimes which can be perpetrated on an industrial scale, and crimes traditionally committed in an offline environment are increasingly being transitioned to an online environment.**Falgun Rathod**,Today's society is highly networked. Internet is ubiquitous and world without it is just inconceivable. As is rightly said that there are two sides of a coin, this blessing in form of ease in access to world of information also has a flip side to it. Devils are lurking in dark to work their stealth. Each click of button takes you closer to them. Recent surveys have shown a phenomenal rise in cyber crime with in short span. Today, cyber crime is just not restricted to e mail hacking but has dug its claws in each e-interaction, producing demons like call spoofing, credit card fraud, child pornography, phishing, remote key logging etc.**K.Jayshankar**Victimization through the Internet is becoming more prevalent as cyber criminals have developed more effective ways to remain anonymous. And as more personal information than ever is stored on networked computers, even the occasional or non-user is at risk. A collection of contributions from worldwide experts and emerging researchers, Cyber Criminology: Exploring Internet Crimes and Criminal Behavior explores today's interface of computer science, Internet science, and criminology.

RESEARCH QUESTION:

Whether cyber crime victims are given importance and help?

Hypothesis:

Null hypothesis:

There is no significant law for the protection of cybercrime victims

Alternative hypothesis:

There is significant law for the protection of cybercrime victims.

MATERIALS AND METHOD:

The have a look at is achieved to discover the impact of schooling at the exercise of casteism is based totally on number one information and secondary statistics.The number one facts for the take a look at modified into collected from 1597 pattern respondents,selected in a random way.The secondary information for the study became gathered from journals, newspaper articles and laws associated with indebtedness. The look at used a survey questionnaire to collect the facts and we used percent assessment for a meaningful assessment.The present study deals with analytical research and descriptive study. Data for this research is collected from primary and secondary sources . Data collection methods are .Books and articles ,Magazines ,Journals and Research articles.The dependent variable is age and the independent variable is importance to cybercriminals victims .

Analysis:

Table:1 Cyberattack and victims

Whether there are laws to protect the victims of cyber attack

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	882	55.2	55.2	55.2
	no	715	44.8	44.8	100.0
	Total	1597	100.0	100.0	

Count

		Whether there are laws to protect the victims of cyber attack		
		yes	no	Total
age	below 20	177	49	226
	21-30	190	328	518
	31-40	157	179	336
	41-50	149	153	302
	above 50	209	6	215
Total		882	715	1597

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	288.110[a]	4	.000
Likelihood Ratio	341.463	4	.000
Linear-by-Linear Association	37.828	1	.000
N of Valid Cases	1597		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 96.26.

Symmetric Measures

		Value	Asymptotic Standardized Error[a]	Approximate T[b]	Approximate Significance
Interval by Interval	Pearson's R	-.154	.023	-6.223	.000[c]
Ordinal by Ordinal	Spearman Correlation	-.129	.025	-5.182	.000[c]
N of Valid Cases		1597			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Based on normal approximation.

age * Do you think the laws for cyber attack on women is sufficient

Table:2 Do you think the laws for cyber attack on women is sufficient

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	630	39.4	39.4	39.4
	no	967	60.6	60.6	100.0
	Total	1597	100.0	100.0	

Crosstab

Count

		Do you think the laws for cyber attack on women is sufficient		
		yes	no	Total
age	below 20	84	142	226
	21-30	207	311	518
	31-40	200	136	336
	41-50	125	177	302
	above 50	14	201	215
Total		630	967	1597

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	155.360[a]	4	.000
Likelihood Ratio	180.189	4	.000
Linear-by-Linear Association	26.944	1	.000
N of Valid Cases	1597		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 84.82.

Symmetric Measures

		Value	Asymptotic Standardized Error[a]	Approximate T[b]	Approximate Significance
Interval by Interval	Pearson's R	.130	.023	5.233	.000[c]
Ordinal by Ordinal	Spearman Correlation	.103	.024	4.138	.000[c]
N of Valid Cases		1597			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Based on normal approximation.

DISCUSSION:

It can be observed from table 1.1 that the Percentage of number of people below 20 who have responded for the survey questions is 14.2% and between 21-30 years are around 32.4% people have responded.within the age group of 31-40 years are 21.9% of people have responded.Finally people from 41-50 years 18.9% of people have responded for the survey and above 50 years is 13.5%. since the person table 4 and table 5 chi square value is 0.000 is greater than 0.05,there is a relationship between dependent variable and independent variable.Hence the null hypothesis is proved Therefore there is no significant law for protection of cybercrime victims..when we asked about the laws protecting women from cyber attack are sufficient among 1500 respondents 652 yes and 967 members say no .

CASE LAW ANALYSIS:

Kalandi Charan Lenka Vs. State of Odisha – In this, the petitioner was continuously being stalked, and a fake account of her was later created and obscene messages were sent to the friends by the culprit. A morphed naked picture was also posted on the walls of the hostel where the victim stayed. The court held the culprit liable for his offence.

Rajiv Dinesh Gadkari through **P.A. Depamala Gadkari vs Smt. Nilangi Rajiv Gadkari** – In this case, after receiving a divorce letter from her husband, the respondent filed a suit against the husband for continuously harassing her by uploading vulgar photographs and defaming her. The offence

has already been registered and maintenance of Rs. 75,000 per month has been claimed by the wife(respondent).In the case of **SMC Ltd. V. Jogesh Kwatra,** derogatory remarks were sent by the employee to the employers and other subsidiaries of the company, and they have been restrained by Delhi High Court from carrying any kind of communication to the plaintiff. This order of Delhi High Court was presumed to be of great significance as it was the first time that an Indian court assumes jurisdiction in a case of cyber defamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiff by disallowing him to send any derogatory, abusive and obscene emails to the plaintiff. Further, the employer was not held vicariously liable as the defendant was not acting as a part of his employment and was off on a frolic of his own.

RECOMMENDATIONS:

- Cyber crime victims should want to be given space to overcome the problem
- Government should want to help them overcome the problems faced by them due to the cyberattack
- The laws on protection of women from cyberattacks should be given importance because they are attacked mostly and been subjected heavy cruelty such as pronography,morphing, etc are increasing.
- Government should consider about cyber issues and want to curb it from the future by implementing strict punishments.

CONCLUSION:

The cyber attacks are becoming more popular and dangerous it may be an attack on a person or group or society but the laws as on cyber crime and attacks towards safety of women ,children and tenagers should be protected.the cybercrime victims should get attention and we'll treatment we should want to provide them mentally overcome the issues and give them a better deserved life.the laws should want to be strengthened and strictly enforced to stop cybercrime

PAPERPILE:

1. Abidi, D.S.S.H. & Abidi, S.S.H., 2018. Cyber Crimes in India: Judicial Endeavours. *LAW REVIEW*, 38(1). Available at: http://dx.doi.org/10.29320/jnpglr.38.1.7.
2. Anon, 2016. Sex Trafficking in Gujarat, India: Case Studies of Women Victims Turned Offenders. *Interpersonal Criminology*, pp.177–189. Available at: http://dx.doi.org/10.1201/9781315368528-1
3. Brown, S.E., Esbensen, F.-A. & Geis, G., 2018. Crimes Without Victims and Victims Without Crimes. *Criminology*, pp.469–504. Available at: http://dx.doi.org/10.4324/9780429469909-13.
4. Damle, P., 2012. "Psychology for Crime Free India - A Focus on Cyber Crimes." *PsycEXTRA Dataset*. Available at: http://dx.doi.org/10.1037/e670282012-047.
5. Deshpande, D.A.M.N. et al., 2018. A Brief Study on Cyber Crimes and IT Act in India. *International Journal of Trend in Scientific Research and Development*, Special Issue(Special-ICDEBI2018), pp.141–149. Available at: http://dx.doi.org/10.31142/ijtsrd18693.
6. Djanggih, H., 2018. THE PHENOMENON OF CYBER CRIMES WHICH IMPACT CHILDREN AS VICTIMS IN INDONESIA. *Yuridika*, 33(2), p.212. Available at: http://dx.doi.org/10.20473/ydk.v33i2.7536.
7. Fatima, H., Dash, G.N. & Pradhan, S.K., 2017. Soft Computing applications in Cyber crimes. *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*. Available at: http://dx.doi.org/10.1109/anti-cybercrime.2017.7905265.
8. Gandhi, B.M. & India, 2006. *Indian Penal Code*,
9. Graham, N., 2018. Cyber crimes against women in India. *Asian Journal of Women's Studies*, 24(3), pp.413–417. Available at: http://dx.doi.org/10.1080/12259276.2018.1496783.
10. Halder & Debarati, 2011. *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations: Laws, Rights and Regulations*, IGI Global.
11. Halder, D. & Jaishankar, K., 2016. *Cyber Crimes against Women in India*, SAGE Publications India.
12. Imran, M., Emerging Trends in Cyber Crimes in India: An Over View. *SSRN Electronic Journal*. Available at: http://dx.doi.org/10.2139/ssrn.2818402.
13. Jaishankar, K., 2011. *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, CRC Press.
14. Khan, M.A., Pradhan, S.K. & Fatima, H., 2017. Applying Data Mining techniques in Cyber Crimes. *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*. Available at: http://dx.doi.org/10.1109/anti-cybercrime.2017.7905293.
15. Kravetz, D., 2013. The Protection of Victims in War Crimes Trials. *Victims of International Crimes: An Interdisciplinary Discourse*, pp.149–163. Available at: http://dx.doi.org/10.1007/978-90-6704-912-2_9.
16. Kumar, P.N.V. & Vijaya Kumar, P.N., 2016. Growing cyber crimes in India: A survey. *2016 International Conference on Data Mining and Advanced Computing (SAPIENCE)*. Available at: http://dx.doi.org/10.1109/sapience.2016.7684146.
17. Martellozzo, E. & Jane, E.A., 2017. *Cybercrime and its victims*, Taylor & Francis.
18. Pandey, K., Laws Relating to Cyber Crimes in India. *SSRN Electronic Journal*. Available at: http://dx.doi.org/10.2139/ssrn.2412469.
19. Walleyn, L., 2009. The Prosecution Of International Crimes And The Role Of Victims' Lawyers. *Reparations for Victims of Genocide, War Crimes and Crimes against Humanity*. Available at: http://dx.doi.org/10.1163/ej.9789004174498.i-576.91.
20. Wright, M.F. et al., 2017. Differences in Attributions for Public and Private Face-to-face and Cyber Victimization Among Adolescents in China, Cyprus, the Czech Republic, India, Japan, and the United States. *The Journal of genetic psychology*, 178(1), pp.1–14.